

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年10月10日

出 願 番 号

Application Number:

特願2002-297289

[ST.10/C]:

[JP2002-297289]

出 願 人

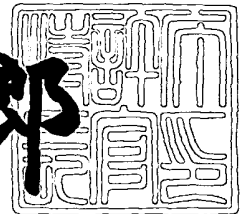
Applicant(s):

松下電器産業株式会社

2003年 6月 5日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3043723

【書類名】 特許願

【整理番号】 2022540407

【提出日】 平成14年10月10日

【あて先】 特許庁長官殿

【国際特許分類】 H04K 1/00
G09C 1/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 太田 雄策

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 松崎 なつめ

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 山内 弘貴

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 布田 裕一

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 グループ登録システムおよびグループ登録端末およびグループ登録要求端末

【特許請求の範囲】

【請求項 1】 グループ登録端末が、グループ登録要求端末を、グループメンバとして登録するグループ登録システムであって、前記グループ登録端末は、他の端末と通信を行うための通信部と、グループ登録要求端末が送信したグループ登録要求情報の正当性を確認する正当性確認部と、登録されているグループメンバの情報を管理するためのグループメンバ管理部とを含み、前記グループ登録要求端末は、他の端末と通信を行うための通信部と、グループ登録要求情報を生成するための登録要求情報生成部とを含み、前記グループ登録要求端末は、前記登録要求情報生成部により、少なくともその情報は有限な時間しか存在できないとする制限情報を含む登録要求情報を生成し、前記通信手段を用いて、前記登録要求情報を送信し、グループ登録端末は、前記通信手段により前記登録要求情報を受信し、前記正当性確認部により、少なくとも前記有限な時間しか存在できないとする制限情報を確認し、その正当性が確認されたときのみ、前記グループ登録要求端末を前記グループメンバ管理部にグループメンバとして登録することを特徴とするグループ登録システム。

【請求項 2】 グループ登録端末とグループ登録要求端末の間で、互いに、登録処理に必要な情報を送受信することを特徴とする請求項 1 記載のグループ登録システム。

【請求項 3】 グループ登録端末とグループ登録要求端末の少なくともどちらか一方は、通信伝送路上に一度に伝送可能な最大の伝送量を探索し、決定する最大伝送量探索部を含み、登録処理のために送受信する情報の情報量は、前記最大伝送量探索部により決定された最大伝送量に等しく、かつ前記情報を分割して伝送することを禁止することを特徴とする請求項 1 または請求項 2 記載のグループ登録システム。

【請求項 4】 グループ登録端末とグループ登録要求端末の少なくともどちらか一方は、登録処理のための情報を中継する機器に固有の情報を取得するための

、中継機器固有情報取得部を含み、登録のために送受信する情報として、送信する機器と受信する機器を中継する機器に固有の情報を内包することを特徴とする請求項 1 または請求項 2 記載のグループ登録システム。

【請求項 5】 グループ登録端末とグループ登録要求端末の少なくともどちらか一方は、端末に固有の情報を管理するための端末固有情報管理部を含み、登録のために送受信する情報として、送信元の端末に固有の情報を内包することを特徴とする請求項 1 または請求項 2 記載のグループ登録システム。

【請求項 6】 グループ登録要求端末の端末固有情報管理部は、前記グループ登録要求端末に接続された記録媒体の固有情報を取得し、前記グループ登録要求端末は前記グループ登録要求端末に接続された前記記録媒体をグループメンバーとして登録要求することを特徴とする請求項 1 または請求項 2 記載のグループ登録システム。

【請求項 7】 グループ登録端末およびグループ登録要求端末は、情報を暗号化あるいは復号化するための暗号処理部を含み、登録処理のために送信する情報の少なくとも一部分は前記暗号処理部により暗号化されており、また登録処理のために受信した情報の少なくとも一部分が暗号化されていた場合は、前記暗号処理部により復号化を行い、登録処理のための情報を送受信することを特徴とする請求項 1 から請求項 6 のいずれか 1 項に記載のグループ登録システム。

【請求項 8】 登録処理のために伝送される情報の有限な時間しか存在できないとする制限情報は、その期間を表す量の単位量に等しいことを特徴とする請求項 1 から請求項 7 のいずれか 1 項に記載のグループ登録システム。

【請求項 9】 グループ登録端末とグループ登録要求端末の少なくともどちらか一方は、登録処理に必要な情報を送信するために必要十分な、有限な時間しか存在できないとする制限を探索し、決定する有効期間探索部を含み、登録処理に必要な情報の、有限な時間しか存在できないとする制限情報として、前記有効期間探索部により決定された制限情報を設定することを特徴とする請求項 1 から請求項 7 のいずれか 1 項に記載のグループ登録システム。

【請求項 10】 有限な時間しか存在できないとする制限情報は、I P v 4 ヘッダの T T Lであることを特徴とする請求項 1 から請求項 9 のいずれか 1 項に

記載のグループ登録システム。

【請求項 1 1】 有限な時間しか存在できないとする制限情報は、I P v 6 ヘッダの Hop Limit であることを特徴とする請求項 1 から請求項 9 のいずれか 1 項に記載のグループ登録システム。

【請求項 1 2】 請求項 1 から請求項 1 1 記載のグループ登録システムにおける、グループ登録端末。

【請求項 1 3】 請求項 1 から請求項 1 1 記載のグループ登録システムにおける、グループ登録要求端末。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、例えば、ネットワークに接続された端末のうち、限定された端末のみをグルーピングするネットワークシステムおよび端末に関する。

【0 0 0 2】

【従来技術】

近年、ネットワークに接続された端末のうち、ある限定された端末のみをグルーピングし、生成されたグループ内での情報の共有や、配信および通信などが行われている。従来、このようなグルーピングの方法としては、例えば、ユーザが予めサーバに端末のホスト I D や I P アドレスなどを手動で登録する方法が利用されてきた。具体的には、サーバのサービスにアクセスできるコンピュータを「hosts.allow」というファイルに手動で登録を行っていた（非特許文献 1 参照）。

【0 0 0 3】

【非特許文献 1】

久米原栄著「Linux ファイアウォール管理者ガイド」ソフトバンク、4.
2. 2 節

【0 0 0 4】

【発明が解決しようとする課題】

ところで、上記のようなグルーピングの方法では、次のような問題があった。

【 0 0 0 5 】

第 1 に、ユーザに登録の作業を課すため、ユーザにとって負担が大きい。ユーザは必ずしもネットワーク技術に精通しているとは限らないので、このようなネットワーク管理作業は可能な限り削減したい。

【 0 0 0 6 】

第 2 に、ユーザが、本来グループ内での情報の共有や配信が望まれないような登録してはいけない端末を、不正に、あるいは過失により登録してしまい、正しいグルーピングの形成が阻害される懸念があった。

【 0 0 0 7 】

そこで本発明は、上記事情を考慮してなされたもので、ネットワークに接続された端末のうち、限定された端末のみを、ユーザに負荷を課すことなくグルーピングするためのグループ登録システムを提供することを目的とする。

【 0 0 0 8 】

また、本発明は、ネットワークに接続された端末のうち、限定された端末のみを、ユーザに負荷を課すことなくグルーピングするためのグループ登録端末を提供することを目的とする。

【 0 0 0 9 】

また、本発明は、ネットワークに接続された端末のうち、限定された端末のみを、ユーザに負荷を課すことなくグルーピングするためのグループ登録要求端末を提供することを目的とする。

【 0 0 1 0 】

また、本発明は、ネットワークに接続された端末に接続された記録媒体のうち、限定された端末に接続された記録媒体のみを、ユーザに負荷を課すことなくグルーピングするためのグループ登録要求端末を提供することを目的とする。

【 0 0 1 1 】

本発明は、ネットワークに接続された端末のうち、限定された端末をグルーピングすることにより、グループ内での情報の共有や配信、通信を実現するグループ登録に特に有効である。

【 0 0 1 2 】

【課題を解決するための手段】

本発明の請求項 1 記載の発明は、グループ登録端末が、グループ登録要求端末を、グループメンバとして登録するグループ登録システムであって、前記グループ登録端末は、他の端末と通信を行うための通信部と、グループ登録要求端末が送信したグループ登録要求情報の正当性を確認する正当性確認部と、登録されているグループメンバの情報を管理するためのグループメンバ管理部とを含み、前記グループ登録要求端末は、他の端末と通信を行うための通信部と、グループ登録要求情報を生成するための登録要求情報生成部とを含み、前記グループ登録要求端末は、前記登録要求情報生成部により、少なくともその情報は有限な時間しか存在できないとする制限情報を含む登録要求情報を生成し、前記通信手段を用いて、前記登録要求情報を送信し、グループ登録端末は、前記通信手段により前記登録要求情報を受信し、前記正当性確認部により、少なくとも前記有限な時間しか存在できないとする制限情報を確認し、その正当性が確認されたときのみ、前記グループ登録要求端末を前記グループメンバ管理部にグループメンバとして登録することを特徴とするグループ登録システムであり、情報に有限な時間しか存在できないとする制限情報を設けることで、この制限された有限な時間内にグループ登録端末に登録要求情報が到達したときのみ、グループピングすることができる、という作用を有する。

【0013】

本発明の請求項 3 記載の発明は、請求項 1 または請求項 2 記載のグループ登録システムにおいて、グループ登録端末とグループ登録要求端末の少なくともどちらか一方は、通信伝送路上に一度に伝送可能な最大の伝送量を探索し、決定する最大伝送量探索部を含み、登録処理のために送受信する情報の情報量は、前記最大伝送量探索部により決定された最大伝送量に等しく、かつ前記情報を分割して伝送することを禁止することにより、グループ登録端末とグループ登録要求端末の間で送受信される情報に、追加的な情報を付加することを防ぐことができる、という作用を有する。

【0014】

本発明の請求項 4 記載の発明は、請求項 1 または請求項 2 記載のグループ登録

システムにおいて、グループ登録端末とグループ登録要求端末の少なくともどちらか一方は、登録処理のための情報を中継する機器に固有の情報を取得するための、中継機器固有情報取得部を含み、登録のために送受信する情報として、送信する機器と受信する機器を中継する機器に固有の情報を内包するにより、グループ登録端末とグループ登録要求端末の間に介在する中継機器が同じであることを証明できる、という作用を有する。

【 0 0 1 5 】

本発明の請求項 5 記載の発明は、請求項 1 または請求項 2 記載のグループ登録システムにおいて、グループ登録端末とグループ登録要求端末の少なくともどちらか一方は、端末に固有の情報を管理するための端末固有情報管理部を含み、登録のために送受信する情報として、送信元の端末に固有の情報を内包することにより、端末に固有な情報を持たない端末は、グループに登録することができない、という作用を有する。

【 0 0 1 6 】

本発明の請求項 6 記載の発明は、請求項 1 および請求項 2 記載のグループ登録システムにおいて、グループ登録要求端末の端末固有情報管理部は、前記グループ登録要求端末に接続された記録媒体の固有情報を取得し、前記グループ登録要求端末は前記グループ登録要求端末に接続された前記記録媒体をグループメンバとして登録要求することにより、記録媒体をグループメンバとして登録することが可能になる、という作用を有する。

【 0 0 1 7 】

本発明の請求項 7 記載の発明は、請求項 1 から請求項 6 のいずれか一項に記載のグループ登録システムにおいて、グループ登録端末およびグループ登録要求端末は、情報を暗号化あるいは復号化するための暗号処理部を含み、登録処理のために送信する情報の少なくとも一部分は前記暗号処理部により暗号化されており、また登録処理のために受信した情報の少なくとも一部分が暗号化されていた場合は、前記暗号処理部により復号化を行い、登録処理のための情報を送受信することにより、登録処理のために送受信する情報の秘匿性を確保することが可能になる、という作用を有する。

【 0 0 1 8 】

本発明の請求項 9 記載の発明は、請求項 1 から請求項 7 のいずれか 1 項に記載のグループ登録システムにおいて、グループ登録端末とグループ登録要求端末の少なくともどちらか一方は、登録処理に必要な情報を送信するために必要十分な、有限な時間しか存在できないとする制限を探索し、決定する有効期間探索部を含み、登録処理に必要な情報の、有限な時間しか存在できないとする制限情報として、前記有効期間探索部により決定された制限情報を設定することにより、動的な、有限な時間しか存在できないとする制限情報の決定が可能になる、という作用を有する。

【 0 0 1 9 】

【発明の実施の形態】

以下、本発明の実施の形態について、図 1 から図 1 4 を用いて詳細に説明する。

【 0 0 2 0 】

(実施の形態 1)

<概要>

本実施の形態において、登録要求端末からの登録要求情報は IP (Internet Protocol) パケットの形式で送信される。IP のバージョンとしては、例えば IPv4 (Internet Protocol Version 4) を使用する。登録要求情報の、有限な時間しか存在できないとする制限情報としては IP ヘッダ内にある TTL (Time To Live) フィールドを利用する。

【 0 0 2 1 】

具体的には、登録要求端末は登録端末に対し、TTL (Time To Live) の値が 1 である登録要求パケットを送信する。TTL が 1 であるため、この登録要求パケットはルータにより転送されることはなく、1 台のルータの下に登録要求端末と登録端末が存在するときのみ、登録端末は登録要求パケットを受信する。登録端末は登録要求パケットを受信すると、TTL の値を確認し、送信元機器をグループメンバとして登録する。

【 0 0 2 2 】

このように、登録端末はTTLを情報の、有限な時間しか存在できないとする制限情報として利用することにより、登録要求端末の認証を行う。

【 0 0 2 3 】

なお、上述のIP v 4、IPパケット、IPヘッダおよびTTLの各用語は例えばRFC (Request For Comment) 791にて説明されている。

【 0 0 2 4 】

<構成>

図1は本実施の形態における登録端末、登録要求端末およびルータの接続図である。図1に示すように、グループはルータ0110に接続される登録端末0111と登録要求端末0112からなる。実際には登録要求端末は登録要求端末0112以外に複数台接続されることもあるが、本説明においては簡単のため省略している。またルータ0110はルータ0101に接続される。同様にルータ0101に接続されるルータ0120があり、ルータ0120には非グループメンバである登録要求端末0121と0122が接続されている。図1のネットワークでは、通信はIPパケットの形式で実施される。図1の場合、登録要求端末0112は登録端末0111にグループメンバとして登録されるが、登録要求端末0121および登録要求端末0122はグループメンバとして登録されない。この機構については後に説明する。

【 0 0 2 5 】

登録要求端末0112、登録要求端末0121および登録要求端末0122は例えばネットワークへの接続が可能な家電製品などである。

【 0 0 2 6 】

登録要求端末0112は、自身が登録端末0111が管理するグループの正当なメンバであることを、TTL値が1の登録要求パケットを登録端末0111に送信することにより証明する。すなわち、一般にTTL値が1のパケットはルータにより他のネットワークに転送することが禁止されているため、この登録要求パケットは、登録端末と登録要求端末が同じルータの下に接続されているときの

み登録端末0111に到達する。また、図1における登録要求端末0121や登録要求端末0122は、登録端末0111に登録要求パケットを到達させるためには、TTL値が少なくとも4以上の値のパケットを送信する必要があり、TTL値が1の登録要求パケットは登録端末0111に到達不可のため、グループへの参加ができない。

【0027】

なお、図1では登録端末0111、登録要求端末0112はルータ0101に直接接続されている場合の例を示したが、本実施の形態は必ずしもこの構成に限定されるものではなく、例えば、間にスイッチやハブなどを介して接続されていても同様の効果が得られる。

【0028】

以上の機構を実現するための登録端末および登録要求端末の構成と動作を以下に詳細に説明する。

【0029】

図2は登録端末0200の構成を示す図である。登録端末0200は通信部0201、正当性確認部0202、確認情報生成部0203、グループメンバ管理部0204および端末固有情報管理部0205から構成される。

【0030】

通信部0201はルータなどを介して他端末と通信をする際のインターフェースである。送信用の最終的なIPパケットはここで生成され、受信用IPパケットはここから受信する。

【0031】

正当性確認部0202は、登録要求端末から受信したIPパケットのIPヘッダを解析し、TTL値が確かに1であることを確認する。

【0032】

確認情報生成部0203は、登録要求端末からの登録端末検索パケットを受信した後に、送信元の登録要求端末に自身に関する情報を通知し、また送信元を確認するための情報を生成する。具体的な情報の形式例は、図4に確認情報パケット0402として図示されるように、自身の機器IDや送信元登録要求端末の機

器IDをIPペイロードとして内包されており、TTLが1に設定されている。生成された確認情報パケットは通信部0201を介して送信元登録要求端末に送信される。

【0033】

グループメンバ管理部0204は、正当性確認部0202が登録要求端末から受信した登録要求パケットの正当性を確認した後、登録要求パケットに内包される登録要求端末の端末IDを、登録端末0200が管理するグループのメンバIDとして登録し、管理する。

【0034】

端末固有情報管理部0205は、自身の機器IDやIPアドレス、MACアドレスに関する情報を管理する。

【0035】

図3は登録要求端末0300の構成を示す図である。登録要求端末0300は通信部0301、登録要求情報生成部0302、登録端末検索情報生成部0303および端末固有情報管理部0304から構成される。

【0036】

通信部0301および端末固有情報管理部0304は、図2における登録端末0200のそれと同様であるので説明を省略する。

【0037】

登録要求情報生成部0302は、登録端末に対し自身をグループメンバとして登録を要求するための情報を生成する。具体的な情報の形式例は、図4に登録要求パケット0403として示されるように、自身の機器IDをIPペイロードに内包し、TTLを1に設定して、登録端末を宛先アドレスに設定する。生成された登録要求パケットは通信部0301を介して登録端末に送信される。

【0038】

登録端末検索情報生成部0303は、自身と同じネットワーク内に登録端末が存在するか否かを検索するための情報を生成する。具体的な情報の形式例は、図4に登録端末検索パケット0401として示されるように、TTLの値は1に設定され、宛先アドレスにはマルチキャストアドレスが設定されており、IPペイ

ロードには登録端末検索情報である旨が内包されている。生成された登録端末検索パケットは通信部0301を介してマルチキャスト送信される。

【0039】

<動作>

以上を示した構成をもつ登録要求端末が、登録端末にグループメンバとして登録される場合の動作を以下に説明する。

【0040】

図5は、登録端末0510が登録要求端末0520をグループメンバとして登録する際のフローを図式化したものである。

【0041】

まず、登録要求端末0520は、登録端末検索パケットを生成し(0521)、自身の属するネットワークにマルチキャスト送信する(0522)。

【0042】

登録端末0510は、登録端末検索パケットを受信する(0511)と、そのパケットのTTL値やペイロードに含まれる機器IDなどから正当性を確認し(0512)、確認情報パケットを生成する(0513)。

【0043】

生成された確認情報パケットは、送信元である登録要求端末に向けて送信される(0514)。

【0044】

確認情報パケットを受信した登録要求端末(0523)は、確認情報パケットに含まれる送信元の登録端末のIPアドレスを宛先IPアドレスとして、登録要求パケットを生成し(0524)、送信する(0525)。

【0045】

登録要求パケットを受信した登録端末(0515)は、登録要求パケットのTTL値や機器IDなどから正当性を確認(0516)し、この機器IDをグループメンバ情報をしてメンバ登録処理を行う(0517)。

【0046】

<まとめ>

このように、登録要求端末はTTL値が1の登録要求パケットを登録端末へ送信することにより、登録端末と登録要求端末が同じルータの下に接続されているときのみ、登録処理は自動で成立する。

【0047】

従って登録要求端末の利用者は、登録端末に手動で登録処理を行う必要が無い。また、同じルータに接続されていない登録要求端末の登録要求は、TTL値が1のパケットを送信しているため、登録端末に到達することができず、登録処理が成立しない。

【0048】

なお、本実施の形態では、TTL値が1のパケットを送受信することにより、登録処理を行うこととしたが、TTL値は必ずしも1に限定されるものではなく、例えば予め値（例えば10）を定めておき、到達したパケットのTTL値がその値からの増減が無いか、を確認する方法でも、同様の効果は得られる。

【0049】

またなお、本実施の形態では、登録要求端末は登録要求パケットに自身の機器IDを内包するとしたが、必ずしもこの方法に限定されるわけではなく、例えば、登録要求端末に接続された記録媒体の機器IDを内包し、記録媒体をグループメンバとして登録要求しても良い。

【0050】

またなお、本実施の形態では、プロトコルとしてIPv4を使用する例を示したが、必ずしもこのプロトコルに限定されるものではなく、情報に、有限な時間しか存在できないとする制限情報が設けられるようなプロトコルであれば同様の効果が得られる。具体的な他の例としては、例えばIPv6における、Hop Limitフィールドの利用が挙げられる。IPv6については例えばRFC2460にその詳細が説明されている。またなお、本実施の形態では、有限な時間しか存在できないとする制限情報として、TTL値を使用する例を示したが、必ずしもこのTTL値に限定されるものではなく、他の具体例としては、有限な時間しか存在できないとする制限情報として、日付や時間を表すタイムスタンプを利用する方法が挙げられる。この場合、正当性確認部はタイムスタンプ値を確認

し、実際の日付を超過していない場合のみ、この情報を正当な情報として認証する方法が挙げられる。

【0051】

(実施の形態2)

<概要>

本実施の形態においては、実施の形態1で述べた方法において、各生成パケットに、中継機器（具体的にはルータ）に関する固有情報（具体的にはMACアドレス）を加え、パケットサイズがMTU（Maximum Transmission Unit；伝送路の最大転送サイズ）に等しくなるようにパディングする。また、IPヘッダにおけるDF（Don't Fragment）ビットを有効にし、フラグメントを禁止する。またIPペイロード部分は暗号化し、情報の秘匿性を確保する。

【0052】

以上により、実施の形態1で述べた効果に加えて、さらに次の効果が得られる。

【0053】

すなわち、DFビットを有効にし、フラグメント禁止の状態でパケットサイズをMTUに等しくして送信することにより、伝送系路上のその他の端末・機器により、IPパケットに不必要な情報を付加して転送されることを防ぐことができる。

【0054】

また、機器IDを暗号化して送信することで、他端末による成り済ましなどの行為を防ぐことができる。

【0055】

また、中継機器（ルータ）に固有な情報（MACアドレス）を暗号化して送信することにより、登録端末と登録要求端末は、各々が確かに同じ中継機器（ルータ）に接続されていることを認識する。

【0056】

<構成>

本実施の形態における登録端末、登録要求端末およびルータの接続関係は実施の形態1と同様である（図1）。

【0057】

本実施の形態における登録端末および登録要求端末の構成と動作を以下に詳細に説明する。

【0058】

図6は登録端末0600の構成を示す図である。登録端末0600は通信部0601、暗号処理部0602、正当性確認部0603、グループメンバ管理部0604、端末固有情報管理部0605、最大伝送量探査部0606、中継機器固有情報取得部0607、および確認情報生成部0608から構成される。

【0059】

通信部0601は実施の形態1におけるそれと同様であるので説明を省略する。

【0060】

暗号処理部0602は、他端末へ送信するIPパケットのIPペイロード部を暗号化し、あるいは通信部から受信した、IPペイロードが暗号化されているパケットの復号処理を行う。暗号アルゴリズムとしては、例えばFIPS（Federal Information Processing Standard）-197で定義される秘密鍵暗号アルゴリズムAES（Advanced Encryption Standard）が用いられる。また、暗号化および復号化のための鍵は各端末が予め共有の値（グローバルシークレットな値）を保有しているとする。なお、この鍵情報は各端末の秘匿領域に保存されているとする。

【0061】

正当性確認部0603は、登録要求端末から受信したIPパケットのIPヘッダを解析し、TTL値が確かに1であることを確認する。また、受信し、復号化したIPペイロードに含まれる中継機器に固有な情報の値をみて、自身と同じ中継機器を介していることを確認する。

【0062】

グループメンバ管理部0604は、正当性確認部0603が登録要求端末から受信した登録要求パケットの正当性を確認した後、登録要求パケットに内包される登録要求端末の端末IDを、登録端末0600が管理するグループのメンバIDとして登録し、管理する。

【0063】

端末固有情報管理部0605は、自身の機器IDやIPアドレス、MACアドレスに関する情報を管理する。

【0064】

最大伝送量探査部0606は、自身が接続されるネットワークの最大伝送量を調査する。具体的には、RFC1191で説明される経路MTU探索の方法を利用する。

【0065】

中継機器固有情報取得部0607は、中継機器に固有な情報を取得する。ここで中継機器とは例えばルータであり、中継機器に固有な情報とは、例えばMACアドレスである。MACアドレスの取得方法としては、例えばRFC826で定められるARP (Address Resolution Protocol) プロトコルを利用する。

【0066】

確認情報生成部0608は、登録要求端末からの登録端末検索パケットを受信した後に、送信元の登録要求端末に自身に関する情報を通知し、また送信元を確認するための情報を生成する。具体的な情報の形式例は、図8に確認情報パケット0802として図示されるように、自身の機器IDや送信元登録要求端末の機器IDをIPペイロードとして内包されており、TTLが1に設定されている。また、IPパケットとしてのサイズがMTUに等しくなるように、予め決められた値（図8では例として0としている）でパディング処理が施されている。生成された確認情報パケットは暗号処理部0602により暗号化され、通信部0601を介して送信元登録要求端末に送信される。

【0067】

図7は登録要求端末0700の構成を示す図である。登録要求端末0700は

通信部0701、暗号処理部0702、登録端末検索情報生成部0704、端末固有情報管理部0705、最大伝送量探査部0706、中継機器固有情報取得部0707、および登録要求情報生成部0708から構成される。

【0068】

通信部0701、暗号処理部0702、端末固有情報0705、最大伝送量探査部0706、中継機器固有情報取得部0707は、図6における登録端末0600のそれらと同様であるので説明を省略する。

【0069】

登録端末検索情報生成部0704は、自身と同じネットワーク内に登録端末が存在するか否かを検索するための情報を生成する。具体的な情報の形式例は、図8に登録端末検索パケット0801として示されるように、TTLの値は1に設定され、宛先アドレスにはマルチキャストアドレスが設定されており、IPペイロードには、中継機器のMACアドレスや登録端末検索情報である旨が内包されている。生成された登録端末検索パケットは通信部0701を介してマルチキャスト送信される。

【0070】

登録要求情報生成部0708は、登録端末に対し自身をグループメンバとして登録を要求するための情報を生成する。具体的な情報の形式例は、図8に登録要求パケット0803として示されるように、自身の機器ID、中継機器のMACアドレスをIPペイロードに内包し、IPパケットとしてのサイズがMTUに等しくなるようにパディング（図8では例として0としている）し、TTLを1に設定して、登録端末を宛先アドレスに設定する。生成された登録要求パケットは、暗号処理部0702により暗号化され、通信部0701を介して登録端末に送信される。

【0071】

<動作>

以上を示した構成をもつ登録要求端末が、登録端末にグループメンバとして登録される場合の動作を以下に説明する。

【0072】

図9は、登録端末0910が登録要求端末0950をグループメンバとして登録する際のフローを図式化したものである。

【0073】

まず、登録要求端末0950は、中継機器固有情報を取得し(0951)、登録端末検索パケットを生成(0952)する。生成された登録端末検索パケットは暗号化され(0953)自身の属するネットワークにマルチキャスト送信する(0954)。

【0074】

登録端末0910は、登録端末検索パケットを受信する(0911)と、復号化し(0912)、そのパケットのTTL値や、自身が取得した中継機器固有情報(0913)とペイロードに含まれる中継機器固有情報、機器IDなどから正当性を確認し(0914)、確認情報パケットを生成する(0915)。

【0075】

生成された確認情報パケットは、暗号化され(0916)、送信元である登録要求端末に向けて送信される(0917)。

【0076】

確認情報パケットを受信した登録要求端末(0955)は、復号化し(0956)、確認情報パケットに含まれる送信元の登録端末のIPアドレスを宛先IPアドレスとして、登録要求パケットを生成し(0957)、暗号化して(0958)送信する(0959)。

【0077】

登録要求パケットを受信した登録端末(0918)は、復号化し(0919)、登録要求パケットのTTL値や中継機器固有情報、機器IDなどから正当性を確認(0920)し、この機器IDをグループメンバ情報をしてメンバ登録処理を行う(0921)。

【0078】

<まとめ>

このように、IPペイロードに中継機器に固有の情報および自身の機器IDを含め、IPパケット全体がMTUサイズに等しくなるようにパディングし、IP

ペイロードを暗号化して、IPヘッダにおけるDFビットを有効にして、TTL値を1に設定したIPパケットを送受信することにより、実施の形態1で述べた効果に加えて、伝送系路上のその他の端末・機器により、IPパケットに不必要な情報を付加して転送されることを防ぐことができる。

【0079】

また、機器IDを暗号化して送信することで、他端末による成り済ましなどの行為を防ぐことができる。

【0080】

また、中継機器（ルータ）に固有な情報（MACアドレス）を暗号化して送信することにより、登録端末と登録要求端末は、各々が確かに同じ中継機器（ルータ）に接続されていることを認識する。

【0081】

なお、本実施の形態では、TTL値が1のパケットを送受信することにより、登録処理を行うこととしたが、TTL値は必ずしも1に限定されるものではなく、例えば予め値（例えば10）を定めておき、到達したパケットのTTL値がその値からの増減が無いか、を確認する方法でも、同様の効果は得られる。

【0082】

またなお、本実施の形態では、登録要求端末は登録要求パケットに自身の機器IDを内包するとしたが、必ずしもこの方法に限定されるわけではなく、例えば、登録要求端末に接続された記録媒体の機器IDを内包し、記録媒体をグループメンバとして登録要求しても良い。

【0083】

またなお、本実施の形態では、暗号鍵としてグローバルシークレットな情報を使用するとしたが、必ずしもこの方法に限定されるわけではなく、例えば、事前にゼロ知識証明を利用したチャレンジアドレスポンス型のハンドシェイクを行うことにより、セッション鍵を共有する方法であっても良い。

【0084】

またなお、本実施の形態では、プロトコルとしてIPv4を使用する例を示したが、必ずしもこのプロトコルに限定されるものではなく、情報に有限な時間し

か存在できないとする制限情報が設けられるようなプロトコルであれば同様の効果が得られる。具体的な他の例としては、例えば I P v 6 における、H o p L i m i t フィールドの利用が挙げられる。

【 0 0 8 5 】

またなお、本実施の形態では、有限な時間しか存在できないとする制限情報として、T T L 値を使用する例を示したが、必ずしもこの T T L 値に限定されるものではなく、他の具体例としては、有限な時間しか存在できないとする制限情報として、日付や時間を表すタイムスタンプを利用する方法が挙げられる。この場合、正当性確認部はタイムスタンプ値を確認し、実際の日付を超過していない場合のみ、この情報を正当な情報として認証する方法が挙げられる。

【 0 0 8 6 】

(実施の形態 3)

<概要>

登録要求端末と登録端末の間に複数台の中継機器が介在する場合について、実施の形態 2 の方法を応用する。

【 0 0 8 7 】

具体的には、登録要求端末は登録端末からの応答があるまで、T T L 値を最小値の 1 から 1 ずつ増加させ、登録端末と通信するための必要十分な T T L 値を決定する。

【 0 0 8 8 】

この方法により、登録要求端末と登録端末の間に複数台の中継機器が介在する場合についても、実施の形態 2 で述べた効果が得られる。

【 0 0 8 9 】

<構成>

図 1 0 は本実施の形態における登録端末、登録要求端末およびルータの接続図である。図 1 0 に示すように、グループの境界に位置するルータ 1 0 1 0 に接続される登録端末 1 0 0 1 とルータ 1 0 1 1 に接続される登録要求端末 1 0 2 2、ルータ 1 0 1 2 に接続される登録要求端末 1 0 2 3 からなる。実際には登録要求端末は登録要求端末 1 0 2 2、登録要求端末 1 0 2 3 以外に複数台接続されるこ

ともあるが、本説明においては簡単のため省略している。またルータ1010はルータ1000に接続される。図10のネットワークでは、通信はIPパケットの形式で実施される。登録要求端末1022、登録要求端末1023は例えばネットワークへの接続が可能な家電製品などである。

【0090】

なお、図10では登録端末1001、登録要求端末1022、登録要求端末1023はルータ1010、ルータ1011、ルータ1012に直接接続されている場合の例を示したが、本実施の形態は必ずしもこの構成に限定されるものではなく、例えば、間にスイッチやハブなどを介して接続されていても同様の効果が得られる。

【0091】

本実施の形態における登録要求端末の構成と動作を以下に詳細に説明する。なお、登録端末の構成は、実施の形態2におけるそれと同様であるので説明は省略する。

【0092】

図11は登録要求端末1100の構成を示す図である。登録要求端末1100は、図7の構成における登録端末検索情報生成部0704が、有効期間探査部1104に置き換えられた構成となっている。

【0093】

本実施の形態における登録端末の中継機器固有情報取得部0607および登録要求端末1100の中継機器固有情報取得部1107は、登録端末0600が接続されている中継機器のIPアドレスを取得するとする。この値は、利用者が既知であり、登録端末0600および登録要求端末1100には予めその値が設定されているものとする。

【0094】

有効期間探査部1104は、図12に示される有効期間探索パケット1200を生成し、マルチキャスト送信する。この際のTTL値は初めは1である。送信した有効期間探索パケットに対する、登録端末からの応答があるまで、TTLを逐次1ずつ増やしていく。このフローを図式化したのが図13である。まずTT

L 値を 1 に設定して (1301) 有効期間探索パケットを送信する (1302)。端末からの応答が無ければ (1303)、次に TTL 値を最大値 (図 13 では 255) と比較する (1304)。最大値を超えていなければ TTL 値は 1 増加し (1305)、再度有効期間探索パケットを送信する (1302)。

【0095】

以降端末からの応答があるまでこの手順を繰り返し、端末からの応答があった時点での TTL 値を登録処理を行うためのパケットに設定する値として決定する。また、TTL 値が最大値を超えてなお端末からの応答が無い場合は、送信先の端末は存在しないものとして異常終了する (1307)。

【0096】

このように有効期間探索パケットは登録端末検索パケットとしての機能を包含する。

【0097】

なお、上述の説明では TTL 値の最大値を 255 としたが、必ずしもこの値に限定されないことは言うまでもない。

【0098】

中継機器固有情報取得部 1107 および有効期間探査部 1104 以外の各部の動作は、実施の形態 2 におけるそれと同様であるので説明は省略する。

【0099】

<動作>

以上を示した構成をもつ登録要求端末が、登録端末にグループメンバとして登録される場合の動作を以下に説明する。

【0100】

図 14 は、登録端末 1410 が登録要求端末 1450 をグループメンバとして登録する際のフローを図式化したものである。

【0101】

まず登録要求端末 1450 は中継機器固有情報を取得する (1451)。

【0102】

次に有効期間探索パケットを生成し (1452)、暗号化して (1453) マ

ルチキャスト送信する（1454）。

【0103】

以降の処理は実施の形態2と同様であるので説明は省略する。

【0104】

<まとめ>

このように、TTL値を1に限定せず、登録端末が応答を返すまで順次1ずつ増加させ、登録端末と通信するための必要十分なTTL値を決定することにより、実施の形態2で述べた効果に加え、登録端末と登録要求端末の間に複数台のルータが介在する場合においても、グループメンバを自動で登録することができる。

【0105】

なお、本実施の形態では、TTL値が送信先に到達するための必要十分な値であるの packets を送受信することにより、登録処理を行うこととしたが、TTL値は必ずしも前述に限定されるものではなく、例えば予め値（例えば10）を定めておき、到達した packets の TTL 値がその値から先に述べた送信先に到達するための必要十分な値の分だけ減算されているか、を確認する方法でも、同様の効果は得られる。

【0106】

またなお、本実施の形態では、登録要求端末は登録要求 packets に自身の機器IDを内包するとしたが、必ずしもこの方法に限定されるわけではなく、例えば、登録要求端末に接続された記録媒体の機器IDを内包し、記録媒体をグループメンバとして登録要求しても良い。

【0107】

またなお、本実施の形態では、暗号鍵としてグローバルシークレットな情報を使用するとしたが、必ずしもこの方法に限定されるわけではなく、例えば、事前にゼロ知識証明を利用したチャレンジアドレスポンス型のハンドシェイクを行うことにより、セッション鍵を共有する方法であっても良い。

【0108】

またなお、本実施の形態では、プロトコルとしてIPv4を使用する例を示し

たが、必ずしもこのプロトコルに限定されるものではなく、情報に有限な時間しか存在できないとする制限情報が設けられるようなプロトコルであれば同様の効果が得られる。具体的な他の例としては、例えば I P v 6 における、H o p L i m i t フィールドの利用が挙げられる。

【 0 1 0 9 】

またなお、本実施の形態では、有限な時間しか存在できないとする制限情報として、T T L 値を使用する例を示したが、必ずしもこの T T L 値に限定されるものではなく、他の具体例としては、有限な時間しか存在できないとする制限情報として、日付や時間を表すタイムスタンプを利用する方法が挙げられる。この場合、正当性確認部はタイムスタンプ値を確認し、実際の日付を超過していない場合のみ、この情報を正当な情報として認証する方法が挙げられる。

【 0 1 1 0 】

【発明の効果】

以上のように、本発明によれば、ネットワークに接続された端末をグルーピングする際、登録処理に必要な情報に、有限な時間しか存在できないとする制限情報を設定し、この制限された有限な時間内に登録端末に登録要求情報が到達したときのみ、登録要求端末をグループメンバとして登録することにより、ユーザによる登録処理の負荷の無いグループ登録システムが実現できる、という効果が得られる。

【 0 1 1 1 】

また、請求項 3 に係る発明によれば、グループ登録端末とグループ登録要求端末の少なくともどちらか一方は、通信伝送路上に一度に伝送可能な最大の伝送量を探索し、決定する最大伝送量探索部を設け、登録処理のために送受信する情報の情報量は、前記最大伝送量探索部により決定された最大伝送量に等しく、かつ前記情報を分割して伝送することを禁止することにより、グループ登録端末とグループ登録要求端末の間に送受信される情報に、追加的な情報を付加することを防ぐことができる、という効果が得られる。

【 0 1 1 2 】

また、請求項 4 に係る発明によれば、グループ登録端末とグループ登録要求端

末の少なくともどちらか一方は、登録処理のための情報を中継する機器に固有の情報を取得するための、中継機器固有情報取得部を含み、登録のために送受信する情報として、送信する機器と受信する機器を中継する機器に固有の情報を内包するにより、グループ登録端末とグループ登録要求端末の間に介在する中継機器が同じであることを証明できる、という効果が得られる。

【 0 1 1 3 】

また、請求項 5 に係る発明によれば、グループ登録端末とグループ登録要求端末の少なくともどちらか一方は、端末に固有の情報を管理するための端末固有情報管理部を含み、登録のために送受信する情報として、送信元の端末に固有の情報を内包することにより、端末に固有な情報を持たない端末は、グループに登録することができない、という効果が得られる。

【 0 1 1 4 】

また、請求項 6 に係る発明によれば、グループ登録要求端末の端末固有情報管理部は、前記グループ登録要求端末に接続された記録媒体の固有情報を取得し、前記グループ登録要求端末は前記グループ登録要求端末に接続された前記記録媒体をグループメンバとして登録要求することにより、記録媒体をグループメンバとして登録することが可能になる、という効果が得られる。

【 0 1 1 5 】

また、請求項 7 に係る発明によれば、グループ登録端末およびグループ登録要求端末は、情報を暗号化あるいは復号化するための暗号処理部を含み、登録処理のために送信する情報の少なくとも一部分は前記暗号処理部により暗号化されており、また登録処理のために受信した情報の少なくとも一部分が暗号化されていた場合は、前記暗号処理部により復号化を行い、登録処理のための情報を送受信することにより、登録処理のために送受信する情報の秘匿性を確保することが可能になる、という効果が得られる。

【 0 1 1 6 】

また、請求項 9 に係る発明によれば、グループ登録端末とグループ登録要求端末の少なくともどちらか一方は、登録処理に必要な情報を送信するために必要十分な、有限な時間しか存在できないとする制限情報を探索し、決定する有効期間

探査部を含み、登録処理に必要な情報の有限な時間しか存在できないとする制限情報として、前記有効期間探査部により決定された制限情報を設定することにより、動的な、有限な時間しか存在できないとする制限情報の決定が可能になる、という効果が得られる。

【図面の簡単な説明】

【図 1】

実施の形態 1 における、登録端末、登録要求端末およびルータの接続図

【図 2】

実施の形態 1 における、登録端末の構成図

【図 3】

実施の形態 1 における、登録要求端末の構成図

【図 4】

実施の形態 1 における、登録処理の際送受信される情報のフォーマットを示す

図

【図 5】

実施の形態 1 における、登録処理フロー図

【図 6】

実施の形態 2 における、登録端末の構成図

【図 7】

実施の形態 2 における、登録要求端末の構成図

【図 8】

実施の形態 2 における、登録処理の際送受信される情報のフォーマットを示す

図

【図 9】

実施の形態 2 における、登録処理フロー図

【図 10】

実施の形態 3 における、登録端末、登録要求端末およびルータの接続図

【図 11】

実施の形態 3 における、登録要求端末の構成図

【図 1 2】

実施の形態 3 における、有効期間探索パケットのフォーマットを示す図

【図 1 3】

実施の形態 3 における、有効期間探索アルゴリズムを示す図

【図 1 4】

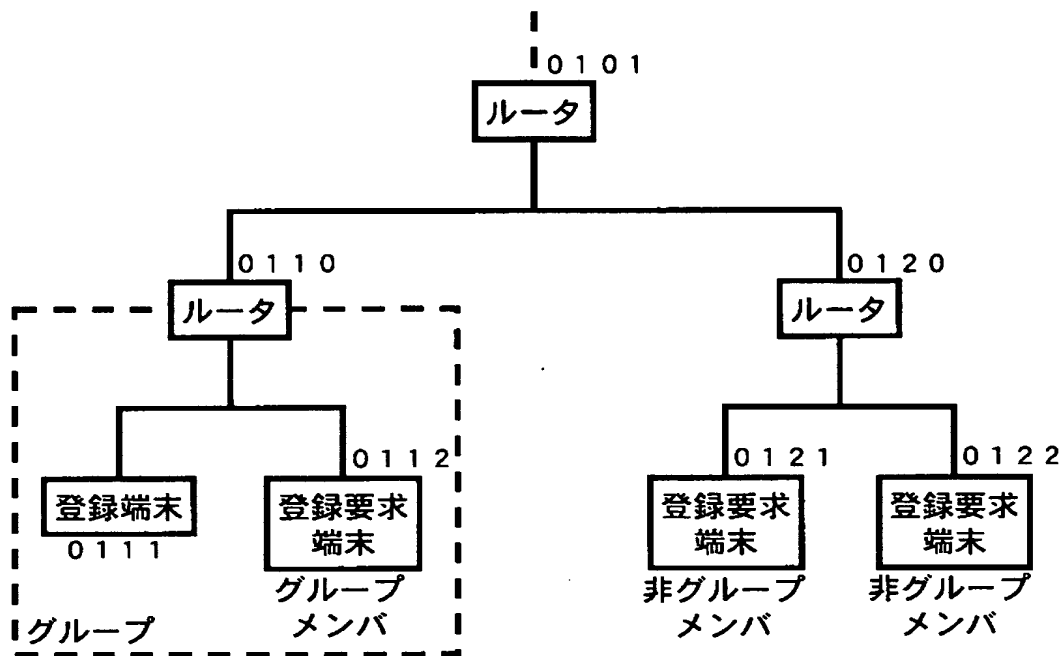
実施の形態 3 における、登録処理フロー図

【符号の説明】

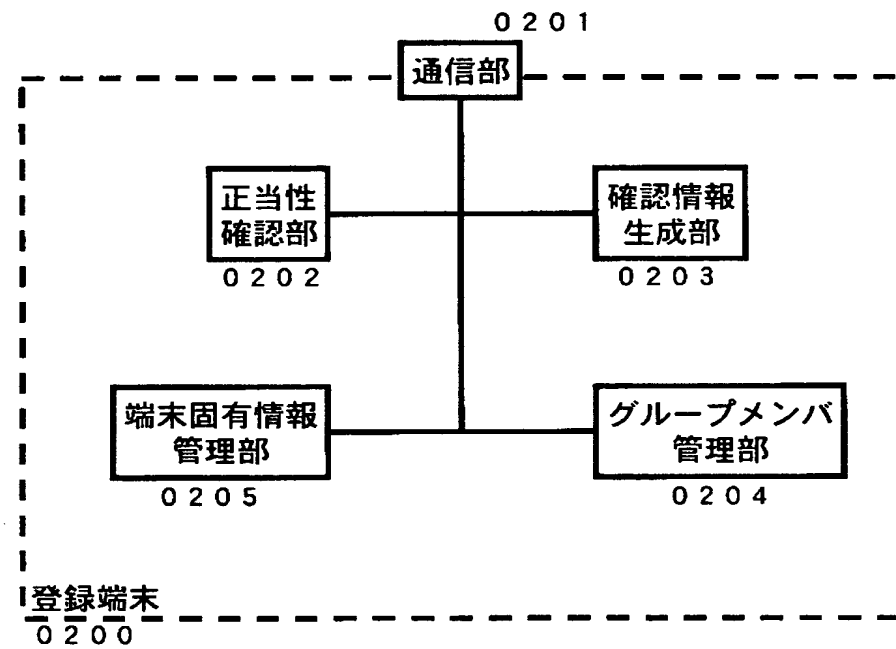
- 0 6 0 1 登録端末の通信部
- 0 6 0 2 登録端末の暗号処理部
- 0 6 0 3 登録端末の正当性確認部
- 0 6 0 4 登録端末のグループメンバー管理部
- 0 6 0 5 登録端末の端末固有情報管理部
- 0 6 0 6 登録端末の最大伝送量探査部
- 0 6 0 7 登録端末の中継機器固有情報取得部
- 0 6 0 8 登録端末の確認情報生成部
- 0 7 0 1 登録要求端末の通信部
- 0 7 0 2 登録要求端末の暗号処理部
- 0 7 0 4 登録要求端末の登録要求端末検索情報生成部
- 0 7 0 5 登録要求端末の端末固有情報管理部
- 0 7 0 6 登録要求端末の最大伝送量探査部
- 0 7 0 7 登録要求端末の中継機器固有情報取得部
- 0 7 0 8 登録要求端末の登録要求情報生成部

【書類名】 図面

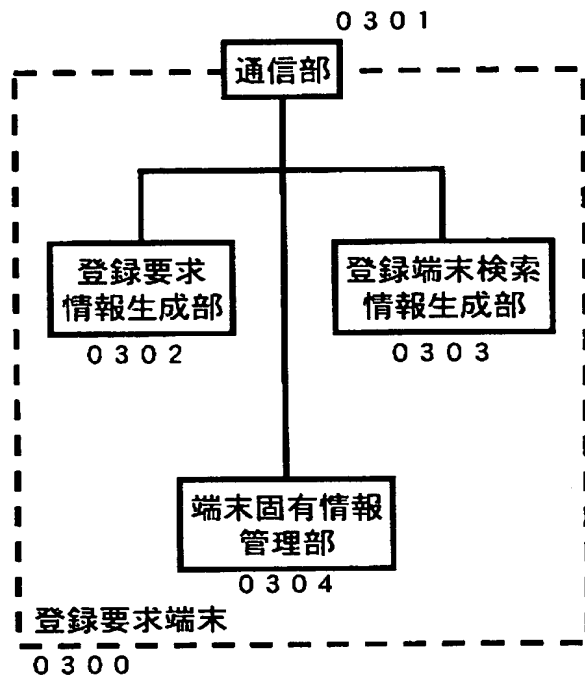
【図 1】



【図 2】



【図3】



【図 4】

登録端末検索パケット 0401

IPヘッダ	TTL	1
	宛先アドレス	マルチキャスト アドレス
IPペイロード	パケット種別	登録端末検索
	機器ID	登録要求端末機器ID 8Byte

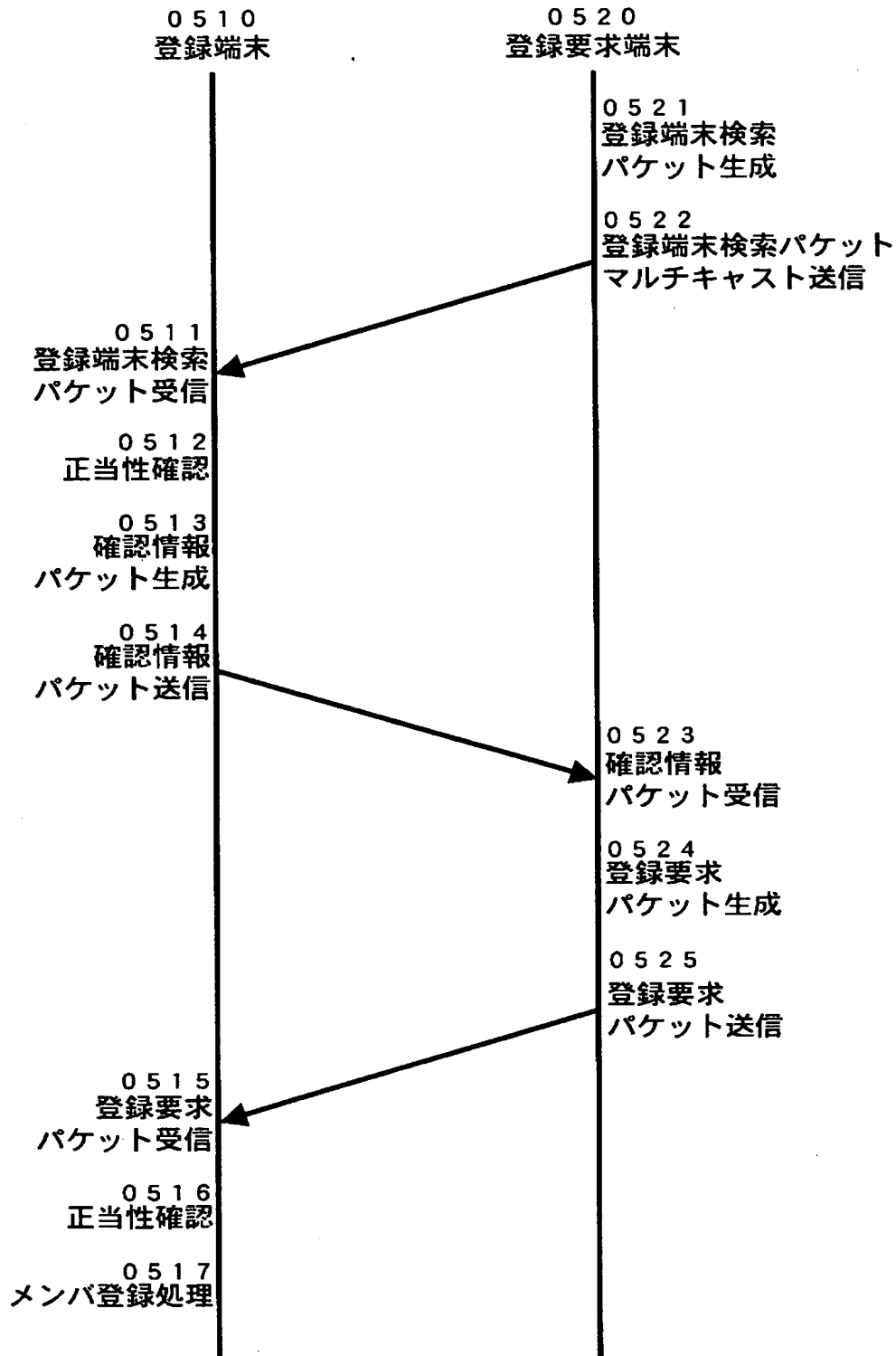
確認情報パケット 0402

IPヘッダ	TTL	1
	宛先アドレス	送信元 登録要求端末
IPペイロード	パケット種別	確認
	登録端末アドレス	IPアドレス

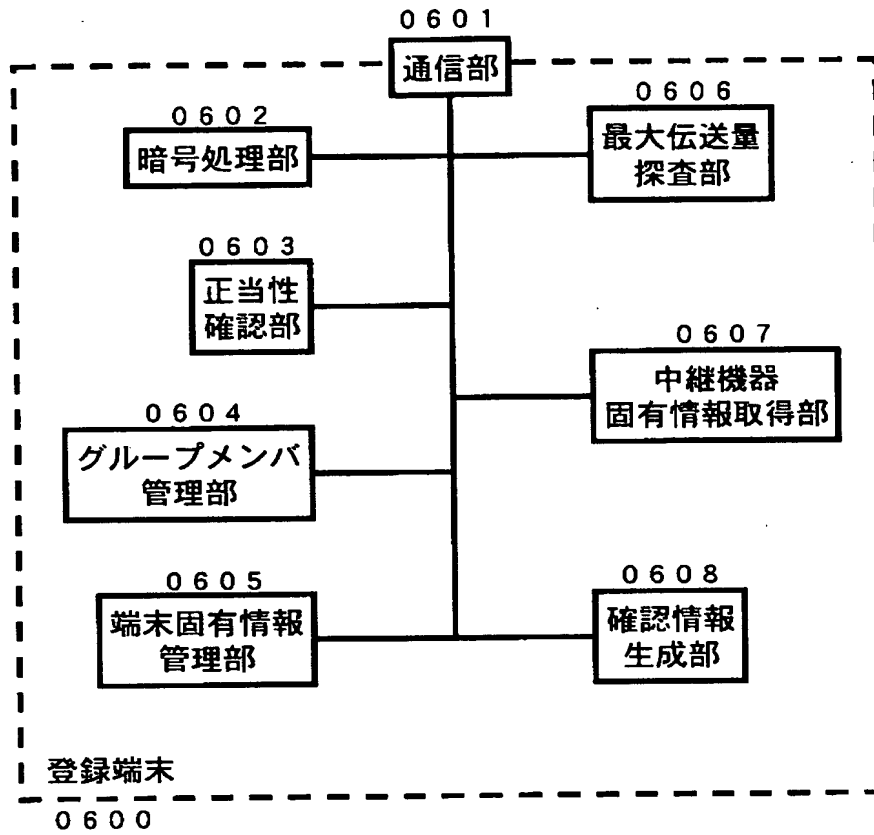
登録要求パケット 0403

IPヘッダ	TTL	1
	宛先アドレス	登録端末
IPペイロード	パケット種別	登録要求
	機器ID	登録要求端末機器ID 8Byte

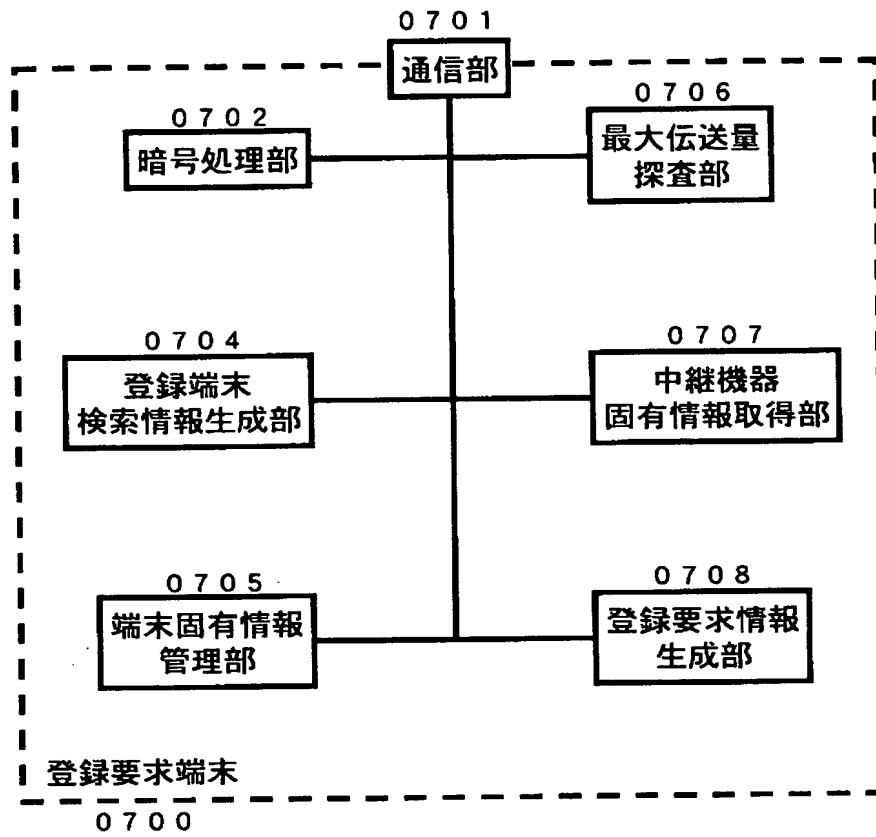
【図5】



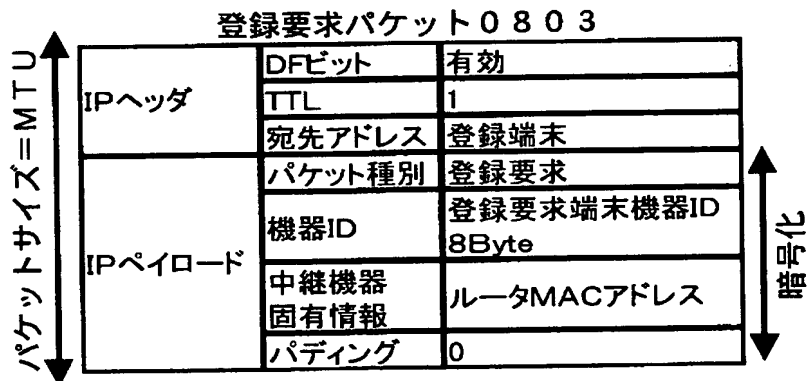
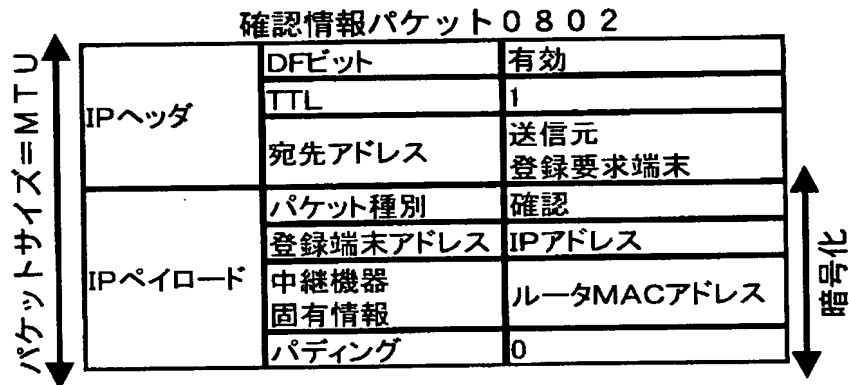
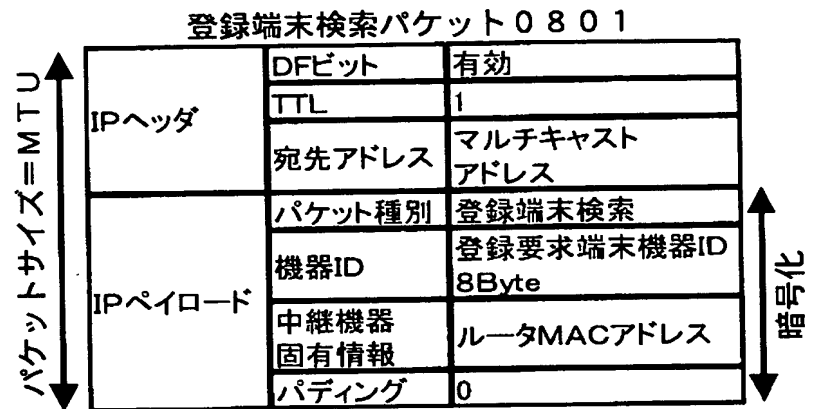
【図 6】



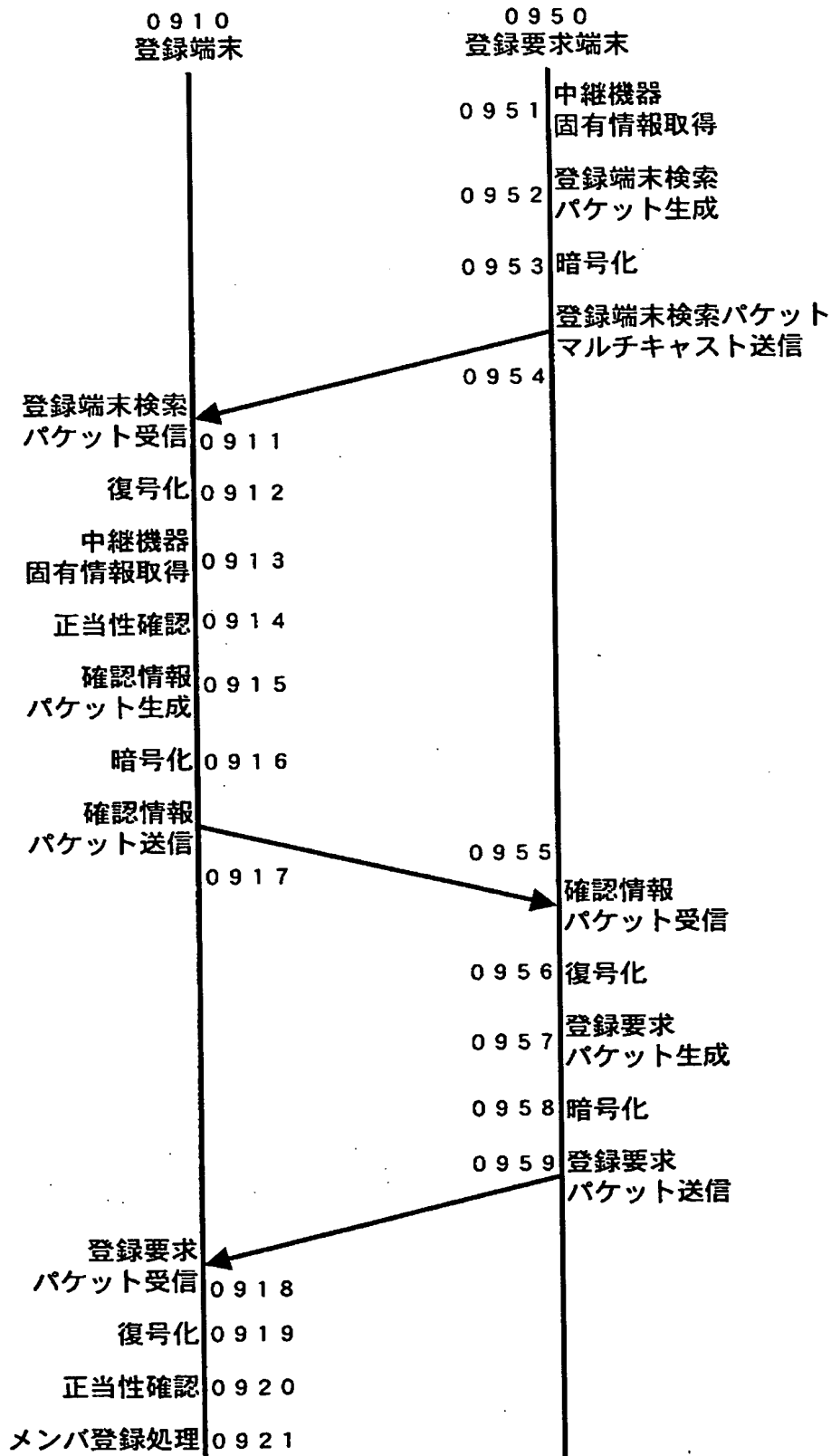
【図 7】



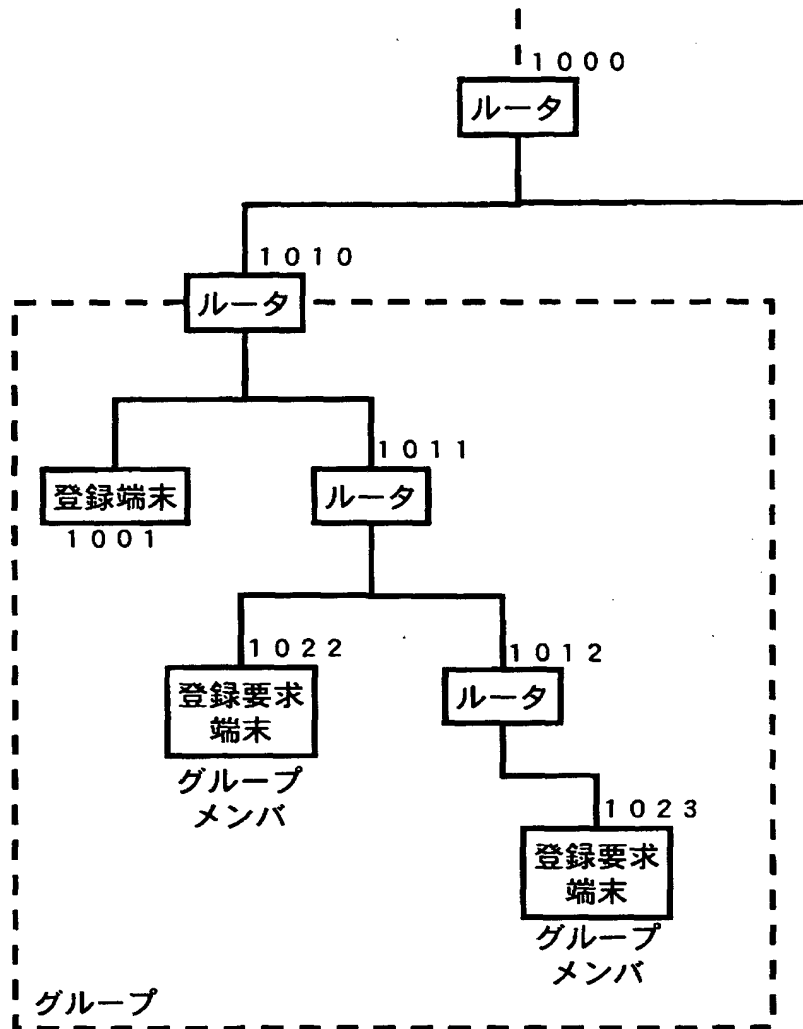
【図 8】



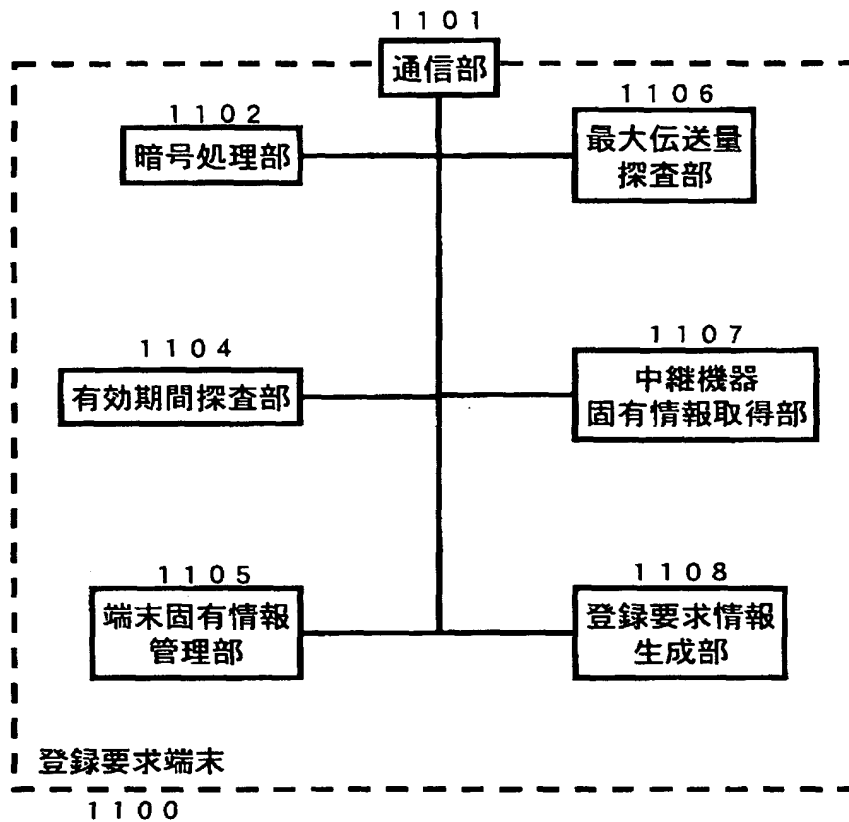
【図9】



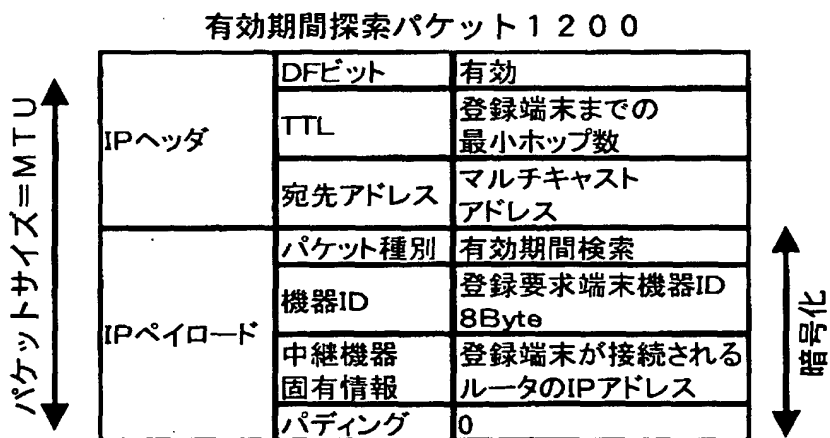
【図10】



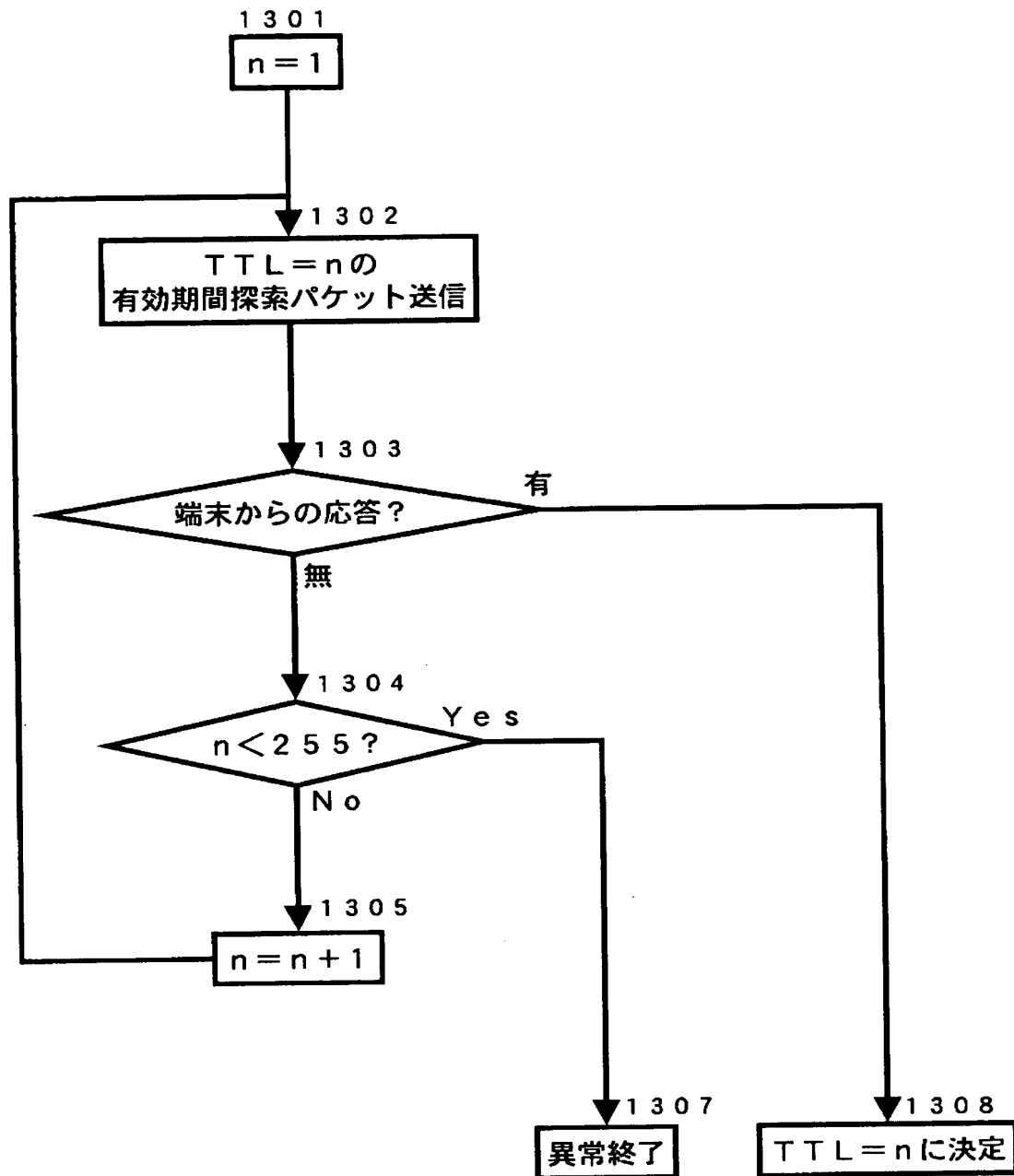
【図11】



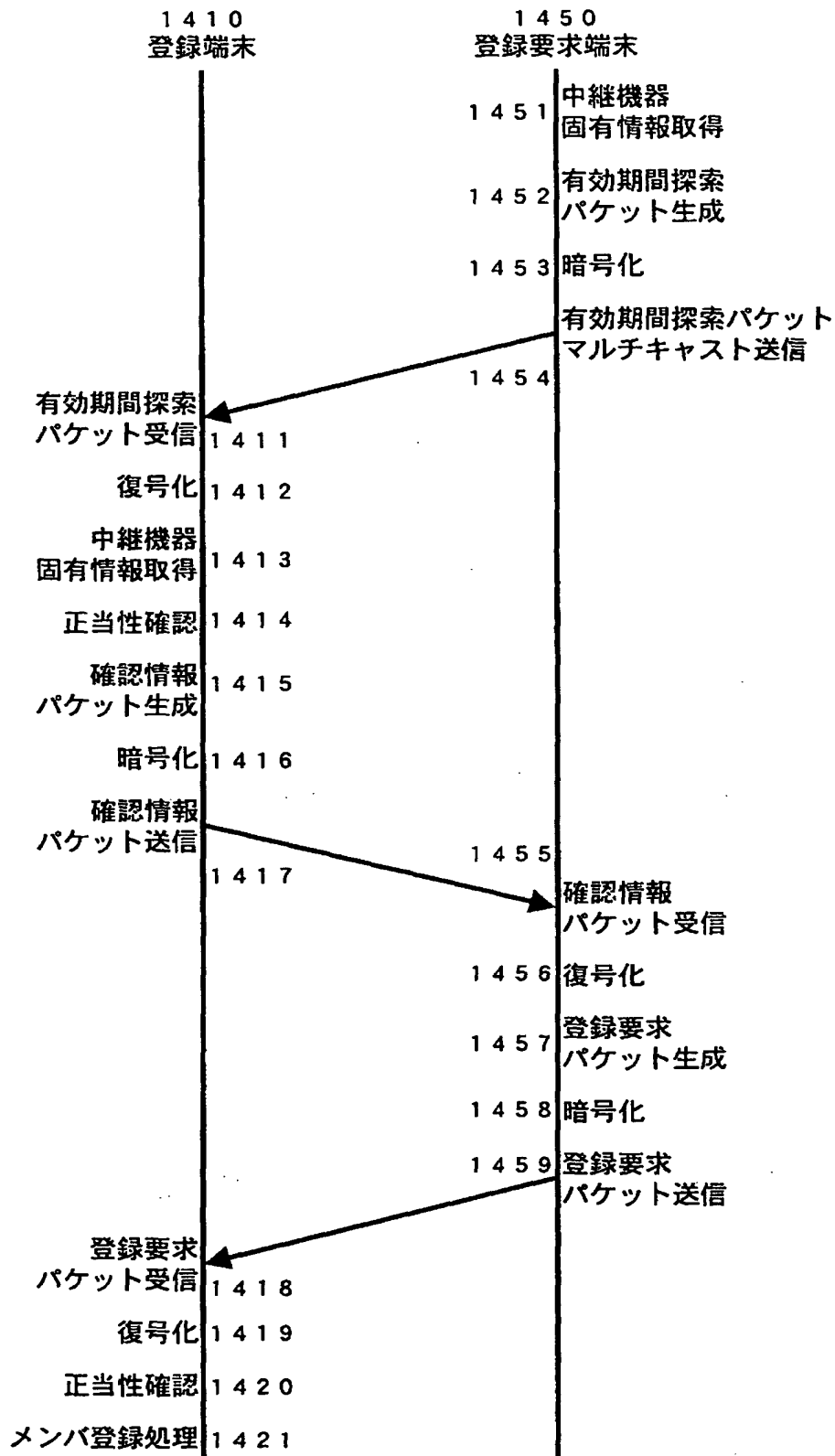
【図12】



【図 13】



【図14】



【書類名】 要約書

【要約】

【課題】 登録処理に必要な情報に、有限な時間しか存在できないとする制限情報を設け、グループ登録端末は、この制限時間内に登録端末に情報が到達する登録要求端末のみをメンバとして登録することにより、ユーザに負荷を課すことなくグルーピングすることが可能なグループ登録システムを提供すること。

【解決手段】 グループ登録要求端末は、登録要求情報生成部により、少なくともその情報は有限な時間しか存在できないとする制限情報に関する情報を含む登録要求情報を生成し、通信手段を用いて登録要求情報を送信し、グループ登録端末は、通信手段により登録要求情報を受信し、正当性確認部により、少なくとも有限な時間しか存在できないとする制限情報を確認し、その正当性が確認されたときのみ、グループ登録要求端末をグループメンバ管理部にグループメンバとして登録する。

【選択図】 図9

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日
[変更理由] 新規登録
住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社